CHAPTER

1 Information Security Overview

There are a few key questions that you need to ask before embarking on any security endeavor. What are you trying to protect? Why are you trying to protect it? How will you protect it? This chapter helps you to address those questions by covering some background information and axioms, ideologies, reasoning, values, and viewpoints you should keep in mind whenever you are considering security tools and techniques. The following sections explain why information is important, the historical context of information protection, methodologies that are used to maximize the effectiveness of security implementations, and how to define and describe the value of the security investment. By keeping these concepts in mind when you refer to this book and when you put this book's practices into operation, you will enhance your success and be able to defend your decisions and choices.

NOTE Words in italics are specialized terms that are defined at the end of this book, in the Security Dictionary. Check the Dictionary for clarification on what these italicized terms mean.

The Importance of Information Protection

Information is an important asset. The more information you have at your command, the better you can adapt to the world around you. In business, information is often one of the most important assets a company possesses. Information differentiates companies and provides leverage that helps one company become more successful than another.

Information can be classified into different categories, as described in Chapter 5. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse. Organizations typically choose to deploy more resources to control information that has higher sensitivity. The U.S. government, for example, uses a five-level classification system that progresses from Unclassified information (which everyone can see) to Top Secret information (to which only the most trusted people have access).

Organizations classify information in different ways in order to differently manage aspects of its handling, such as labeling (whether headers, footers, and watermarks specify how it should be handled), distribution (who gets to see it), duplication (how copies are made and handled), release (how it is provided to outsiders), storage (where it is kept), encryption (if required), disposal (whether it is shredded or strongly wiped), and methods of transmission (such as e-mail, fax, print, and mail). The specifics are spelled out in an organization's information classification and handling policy, which represents a very important component of an organization's overall security policy.

Information intended for internal use only is usually meant to be seen by employees, contractors, and service providers, but not by the general public. Examples include internal memos, correspondence, general e-mail and instant message discussions, company announcements, meeting requests, and general presentation materials. This type of information is typically the least restricted—because spending a lot of time and money on protecting it doesn't outweigh the value of the information or the risk of its disclosure.

Companies may have *confidential information*, such as research and development plans, manufacturing processes, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, financial forecasts, and earnings announcements, that is intended for internal use on a need-to-know basis. Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company. This type of information is available to external audiences only for business-related purposes and only after entering a nondisclosure agreement (NDA) or equivalent obligation of confidentiality.

Specialized information or *secret information* may include trade secrets, such as formulas, production details, and other intellectual property, proprietary methodologies and practices that describe how services are provided, research plans, electronic codes, passwords, and encryption keys. If disclosed, this type of information may severely damage the company's competitive advantage. It is usually restricted to only a few people or departments within a company and is rarely disclosed outside the company.

Egg on Their Faces: A Case Study

Egghead Software was a well-known software retailer who discovered in 2000 that Internet attackers might have stolen as many as 3.7 million credit card numbers from its web site, housed offsite at an e-commerce service provider that lacked good security.

This information quickly made the news, and as a result, Egghead's corporate identity was more than just tarnished—it was destroyed. Customers fled in droves. The media coverage ruined the company's reputation. Egghead's stock price dropped dramatically, along with its sales. Cost-cutting measures, including layoffs, followed. The chain reaction finally concluded with Egghead's bankruptcy and subsequent acquisition by Amazon.com.

Were the consequences of inattention to security too extreme? You be the judge. But could those consequences have been avoided with good security practices? Absolutely.

In some business sectors, the protection of information is not just desirable, it's mandatory. For example, health care organizations are heavily regulated and must comply with the security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). They are required by HIPAA to ensure robust security over *protected health information (PHI)* that consists of medical data and *personally identifiable information (PII)*. Financial institutions are also required by regulations to protect customer information, PII, and financial records. These regulations include security rules defined by the Federal Financial Institutions Examination Council (FFIEC), and the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999. Regulations such as the Sarbanes-Oxley Act of 2002 (also known as SOX or Sarbox) also apply to many companies that are publicly traded, to protect shareholders against the dissemination of false financial information. Other legal regulations include SB 1386 and SB 24, which are California laws requiring companies to protect personal information. All of these regulations carry penalties, some of which are strong, for failure to properly protect information. (Chapter 3 covers these and other regulatory requirements in more detail.) The proliferation of information security regulations around the world is an indicator of the importance of protecting data.

The better your security controls are that protect all these different types of data, the greater the level of access that you can safely provide to authorized parties who need to use that data. Likewise, third parties can give you more access to their data if it's secure. The higher the mutual trust, the more access you can safely provide to external parties such as your customers, suppliers, business partners, vendors, consultants, employees, and contractors. In this global and increasingly digital age, the ability to provide this secure and trusted access is no longer a differentiator, but a business necessity.

The Evolution of Information Security

In the early days of networking, individual computers were connected together only in academic and government environments. Thus, at that time, the networking technologies that were developed were specific to academic and government environments. Originally, the academic security model was "wide open" and the government security model was "closed and locked." There wasn't much in between. The government was mainly concerned with blocking access to computers, restricting internal access to confidential data, and preventing interception of data (for example, by shielding equipment to prevent electromagnetic radiation from being intercepted). This method of protecting assets provided a hard-to-penetrate perimeter, as depicted in Figure 1-1.

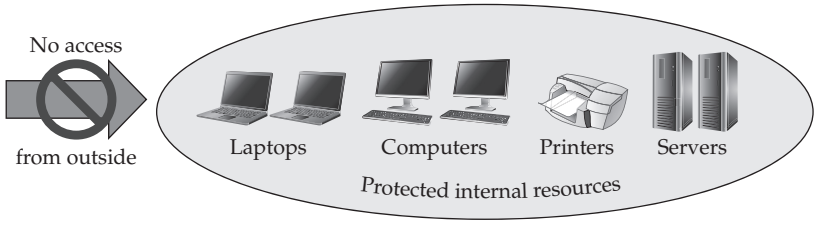

Figure 1-1 Original government perimeter blockade model

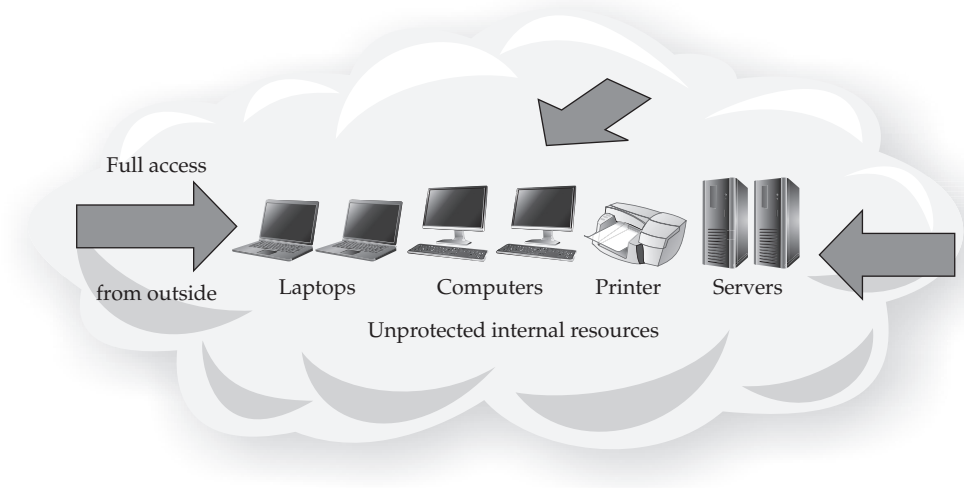

Figure 1-2 Original academic open-access model

In the academic world, the goal was to share information openly, so security controls were limited to accounting functions in order to charge money for the use of computer time. Figure 1-2 shows the original security model for academic institutions. Compare this model with the government model shown in Figure 1-1. Note that these two models are diametrically opposite—the government model blocks everything, while the academic model allows everything. There is plenty of room in between these two extremes.

In the field of computer security, the practices established by the academic and government institutions persisted until the early 1990s, and some of those practices are still around today. Those practices that have endured continue to have their place in a comprehensive security strategy, but they are no longer sufficient to meet the needs of the modern computer network.

Dangers of the Academic Open-Access Model: A Case Study

InterNex was an Internet service provider (ISP) headquartered in Palo Alto, California. The only security control it employed was basic username and password authentication. It had designed its network intentionally to allow unrestricted access. This was a philosophical decision. The ideology of InterNex was that the Internet should be open to everyone.

Unfortunately for InterNex, the open-access philosophy had consequences. Many of its systems were compromised by attackers who were able to guess the passwords of various user accounts. One of the most famous attackers in history, Kevin Mitnick, used InterNex's compromised systems to disguise his identity while attacking other networks, including during the 1994 *IP spoofing attack* against computers in San Diego. Mitnick was eventually captured and served five years in jail.

When businesses started to widely embrace the Internet as a sales channel and business tool in the early-to-mid 1990s, a new security model was required. A closed-door approach doesn't work when you need to allow thousands or millions of people to have access to the services on your network. Likewise, an open-door approach doesn't work when you need to protect the privacy of each individual who interacts with the services on your network. E-commerce and business required a more blended approach of providing limited access to data in a controlled fashion, which is a more sophisticated and complex approach than that used by the earlier security models. To use the analogy of a house, consider the complexity of allowing certain authorized parties (like utility companies, cleaning staff, or caterers) to get into your house while still keeping out burglars and vandals. Isn't it easier just to keep all your doors locked (as in the old government model) or to leave them all unlocked (as in the academic model)? Partial controlled access requires authentication, authorization, and privacy—and more complexity. How would you design the security of a house to provide multilevel, complex, granular access, visibility, and control?

As the use of information technologies evolved, the original all-or-nothing approaches to security no longer met the needs of information consumers. So, the practice of network security evolved. The concepts of intranets and extranets were developed to accommodate internal and external customers, respectively, with secured boundaries that resembled miniature versions of the firewall perimeter. Virtual private networks (VPNs) were developed to provide a secure channel (or tunnel) from one network to another. These approaches continued through the end of the 1990s to the early part of the 2000s, after which the first edition of this book was published in late 2003.

Throughout the first decade of the 21st century, the Internet continued to become an increasingly critical business platform, and the network became more of a key business component. As more companies started doing business on the Internet, concepts such as *Software-as-a-Service (SaaS)* were developed to provide business services over the Internet. And the threats found on the Internet evolved as well. Basic *viruses* and *worms* along with the simple *exploits* and *man-in-the-middle* attacks found in the decade of the 1990s became more sophisticated, effective, and ubiquitous.

Which brings us to today. Business partners need to share information with your company, and often with each other as well. Employees, consultants, contractors, service providers, system integrators, and other entities that augment a company's resources all need to collaborate with a pool of information. The better the distribution vehicle for that information, the more business opportunities that can be accessed by the company. Customers require secure access to the information that they need. A secure data network allows a company to distribute information quickly and effectively throughout the organization, to business partners, and to customers. Figure 1-3 characterizes the interconnectedness among data, computers, networks, and information consumers.

SaaS offerings have become just as prevalent as in-house services—in fact, they are increasingly more prevalent. Companies are choosing to leverage existing service offerings on the Internet rather than build their own. *Social networking* is becoming a powerful marketing force. And *cloud computing* is moving the boundaries of the network even further away from the data center. This global interconnectedness requires a different perspective on security—we can no longer build virtual walls around our networks. Instead, security must be pervasive, built into every aspect of information processing. And the security

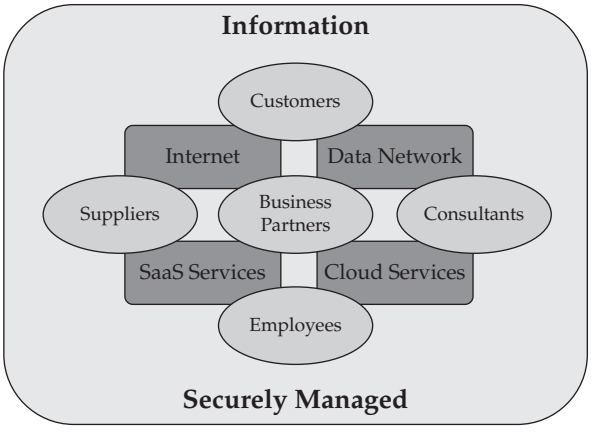

Figure 1-3 Modern information is shared among many consumers, via many channels.

threats to all these information resources have evolved at a rate equal to or greater than the technologies themselves. (Chapter 2 covers modern threats in detail.)

Modern security products are now designed to balance the needs of business on the Internet while protecting against today's sophisticated threats. Modern information security practices have evolved into a blended approach to managing access to information. Technology and information are blended into everyday life, and they can no longer be kept in a locked box or left unprotected.

Justifying Security Investment

How do you justify spending money on security? That is perhaps the most challenging, and debated, topic in the field of information security. First there was FUD—fear, uncertainty, and doubt. Without really measuring anything or delivering specific results, executives were simply frightened into spending money. That didn't last long. Soon thereafter, *return on investment (ROI)* was used as an attempt to market security as an investment that "pays for itself." This was the standard approach to justifying information technology budgets, but it never translated well to security. There is really no good way to demonstrate a monetary amount gained by spending money on security. So, ROI was combined with annualized loss expectancy (ALE), a risk measurement strategy that combines the frequency (or probability) of a loss with the cost of that loss, to produce a yearly expected monetary value. The problem was that too much guesswork went into ALE, and losses don't distribute themselves evenly from year to year, so ALE estimates were really not defensible.

The "insurance analogy" was developed as an alternative to value-based security justifications. People and businesses spend money on insurance—often as much as 10 percent of the value of the asset per year—even though they may never have a claim to file. They spend this money for peace of mind, knowing that they will be covered in the event of a problem. Likewise, businesses spend money on security because it's insurance against

misuse of their assets. How do you measure the value of that insurance? It certainly has value, but it's hard to quantify. The Egghead Software case study presented earlier in this chapter is a good example of how failure to focus on security can cause a major business loss that greatly exceeds the value of the assets themselves.

So, where does that leave us? The business benefits of security are hard to express in terms of a simple monetary value. Instead, consider this justification for security spending: good security practices *enable* business. They allow the business to prosper. They help provide a solid foundation upon which the business can expand and grow. Robust information security practices not only reduce risks and costs, but also provide new opportunities for revenue. In the past, security was thought of only in the context of *protection* (blocking access, closing holes, segmenting and separating systems and networks, and denying connections). Today that view has evolved to focus on enabling business on a global scale, using new methods of communication. By improving access to the information that drives its business, every company can expand its business influence on a global scale, regardless of the company's size or location. Information, one of the important assets a company possesses, is even more valuable when shared with those authorized to have it. Modern security practices provide information to those who need it without exposing it to those who should not have it.

Good security practices allow companies to perform their operations in a more integrated manner, especially with their customers. By carefully controlling the level of access provided to each individual customer, a company can expand its customer base and the level of service it can provide to each individual customer, without compromising the safety and integrity of its business interests, its reputation, and its customers' assets. Specific benefits of a strong security program are business agility, cost reduction, and portability.

Business Agility

Today, every company wants to open up its business operations to its customers, suppliers, and business partners, in order to reach more people and facilitate the expansion of revenue opportunities. For example, manufacturers want to reach individual customers and increase sales through e-commerce web sites. Web sites require connections to back-end resources like inventory systems, customer databases, and material and resource planning (MRP) applications. Extranets need to allow partners and contractors to connect to development systems, source code, and product development resources. And SaaS applications deliver business process tools over the Internet to customers.

Knowledge is power—in business, the more you know, the better you can adapt. Strong security provides insight into what is happening on the network and, consequently, in the enterprise. Weak security leaves many companies blind to the daily flow of information to and from their infrastructure. If a company's competitors have better control of their information, they have an advantage. The protection of a company's information facilitates new business opportunities, and business processes require fewer resources when managed efficiently and securely. Contemporary security technologies and practices make life easier, not harder.

Security allows information to be used more effectively in advancing the goals of organization because that organization can safely allow more outside groups of people to utilize the information when it is secure. The more access you provide, the more people you

can reach—and that means you can do more with less. Automation of business processes, made *trustworthy* by appropriate security techniques, allows companies to focus on their core business. Interconnecting productivity tools opens up new levels of operational effectiveness, and a responsible security program enables that effectiveness without exposure to undue risk.

When all levels of company management strongly support security, have a fundamental knowledge of security principles, and place a high value on security practices, the greatest gain is realized.

Cost Reduction

Modern security practices do reduce some costs, such as those resulting from loss of data or equipment. Data loss due to mishandling, misuse, or mistakes can be expensive. A rampant virus outbreak, a web site outage, or a denial of service (DoS) attack can result in service outages during which customers cannot make purchases and the company cannot transact business. Perhaps even worse, the service outage may attract unwelcome press coverage. The consequences of a security compromise can be significant. A publicized security incident can severely damage the credibility of a company, and thus its ability to acquire and retain customers.

An increasing number of attacks are categorized as *advanced persistent threats (APTs)*. These attacks are designed to deploy malware into a network and remain undetected until triggered for some malicious purpose. Often, the goal of the attacks is theft of financial information or intellectual property. Loss of service or leakage of sensitive data can result in fines, increased fees, and an overall decrease in corporate reputation and stock price. Strong security reduces loss of information and increases service availability and confidentiality.

Portability

Portability means that software and data can be used on multiple platforms or can be transferred/transmitted within an organization, to a customer, or to a business partner. The "consumerization" of information has placed demands on companies to be able to provide meaningful and accurate information at a moment's notice.

A survey of CIOs and CISOs in 2011 concluded that the single biggest driver of information security spending over the preceding three years was client requirement, meaning that customers want to buy products and services from companies that have good security, and will in fact sometimes require evidence of security practices before completing a purchase.

To meet the demands of today's businesses and consumers, architectures and networks need to be designed with security controls baked in as part of the development process. Clearly, this level of broad access to information resources requires a well-thought-out and properly deployed security program. With sound security built in from the ground up, portability of data as a key benefit can be realized.

Portability also enables business and creates value. For example, Apple's ability to both host music and allow personal music libraries to be synchronized to a tablet, mobile phone, and MP3 player has greatly increased Apple's bottom line. Security for mobile platforms affords users the opportunity to take their music everywhere while protecting the interests of the business by preventing unauthorized downloading of copyrighted material.

Security Methodology

Security is a paradigm, a philosophy, and a way of thinking. Defensive failures occur when blind spots exist. A defender who overlooks a *vulnerability* risks the exploitation of that vulnerability. The best approach to security is to consider every asset in the context of its associated *risk* and its value, and also to consider the relationships among all assets and risks.

The field of *security* is concerned with protecting assets in general. *Information security* is concerned with protecting information in all its forms, whether written, spoken, electronic, graphical, or using other methods of communication. *Network security* is concerned with protecting data, hardware, and software on a computer network. The various branches of security are related to each other, to a greater or lesser extent, and this book's techniques apply to all of them. The practices used in this book to approach security provide best results regardless of the branch or specialization—in other words, the basic concepts such as asset identification and valuation, threat definition and risk analysis, and processes and mechanisms to protect assets apply equally well. At its core, the practice of security is all about reducing risks to assets to acceptable levels by using a layered, comprehensive approach so that risk is still mitigated and controlled even when one control fails.

If you're trying to protect a network of computers, a focus only on the security of those computers leads to vulnerabilities and/or risks that attackers might exploit to bypass your protective mechanisms. It is important to consider network security in the context of its relationship to other security fields, as well as to the rest of the enterprise.

CAUTION It is vital to the success of any security endeavor to consider all the factors necessary to successfully integrate security technologies into the enterprise. For example, a firewall cannot be effective without paying attention to its context: the business processes used to support the technology, the assets it is intended to protect, the expected threat vectors, and the adjacent technologies that bypass the firewall. Keep the big picture in mind when wielding technological tools.

The field of information security evolves constantly, but the foundations of good security practice have not changed throughout history. If you are to succeed in protecting your assets, you should consider the lessons learned from successful security strategies, as well as those learned from poor ones. The basic principles apply equally well to any situation or environment, regardless of whether you apply them to defend computers, networks, people, houses, or any other assets.

The Limitations of a Barrier: Case Study

The Maginot Line, a wall built by the French in the 1930s to defend France from invasion by Germany, is one of the most famous defensive failures in history. A strict border defense, it was designed to deny all access from the other side. But the ends of the wall were never finished, lack of maintenance caused it to lose its effectiveness, and changes in warfare technology made blocking human attackers on foot obsolete. The Maginot Line serves as a useful analogy to modern firewalls. Ignoring threats that go around firewalls and failing to properly maintain the firewall platform and configuration can reduce and weaken the firewall's defensive effectiveness.

The basic assumptions of security are as follows:

- We want to protect our assets.
- There are threats to our assets.
- We want to mitigate those threats.

These hold true for any branch of security.

Three aspects of security can be applied to any situation—defense, detection, and deterrence. These are considered the three *D*s of security.

Defense is often the first part of security that comes to mind, and usually it is the easiest aspect for people to understand. The desire to protect ourselves is instinctive, and defense usually precedes any other protective efforts. Defensive measures reduce the likelihood of a successful compromise of valuable assets, thereby lowering risk and potentially saving the expense of incidents that otherwise might not be avoided. Conversely, the lack of defensive measures leaves valuable assets exposed, inviting higher costs due to damage and loss. Defensive controls on the network can include access control devices such as *stateful firewalls* (covered in Chapter 16), *network access control* (covered in Chapters 14 and 15), spam and malware filtering, *web content filtering*, and change control processes (covered in Chapter 31). These controls provide protection from software vulnerabilities, bugs, attack scripts, ethical and policy violations, accidental data damage, and the like. Chapter 2 addresses defense models in more detail. However, defense is only one part of a complete security strategy.

Another aspect of security is *detection*. In order to react to a security incident, you first need to know about it. Examples of detective controls include video surveillance cameras in local stores (or even on your house), motion sensors, and house or car alarm systems that alert passers-by of an attempted violation of a security perimeter. Detective controls on the network include audit trails and log files, system and network intrusion detection and prevention systems (covered in Chapter 18), and security information and event management (SIEM) alerts, reports, and dashboards. A security operations center (SOC) can be used to monitor these controls. Without adequate detection, a security breach may go unnoticed for hours, days, or even forever.

Deterrence is another aspect of security. It is considered to be an effective method of reducing the frequency of security compromises, and thereby the total loss due to security incidents. Many companies implement deterrent controls for their own employees, using threats of discipline and termination for violations of policy. These deterrent controls include communication programs to employees about acceptable usage and security policies, monitoring of web browsing behavior, training programs to acquaint employees with acceptable usage of company computer systems, and employee signatures on agreements indicating that they understand and will comply with security policies. (Chapter 5 covers security policies.) With the use of deterrent controls such as these, attackers may decide not to cause damage.

NOTE Companies that assess their risks and identify what controls and techniques will be most effective against those risks will reap the greatest results. The better security programs will incorporate each of the three *D*s based on how much value each provides in reducing or eliminating the particular risks that are being addressed.

The Illusion of Security: A Case Study

Many drivers of Toyota vehicles in the 1980s were unaware that the door keys for those vehicles had only a small number of variations. They naturally assumed that so many different keys existed, the chance of opening the door of the wrong car was practically impossible. They were wrong. Toyota had so few key variations that thieves were able to carry a full set to steal the cars.

One person who encountered this phenomenon was Betty Vaughn, a retired school teacher in Louisville, Kentucky. Betty returned from a shopping trip to the local mall to find her Toyota's passenger-side mirror broken off and the garage door opener missing. When her husband Edgar arrived home, he noticed the front license plate was also missing. They assumed their car had been vandalized. But wait! The tires were the wrong brand! What kind of vandal would switch their tires? It was then that they checked the glove compartment and discovered from the registration that it wasn't their car. The Vaughns' blue 1992 Toyota Camry had been parked two cars away from Charles Lester's 1993 model. The keys to both vehicles were the same.

This case study appeared in the first edition of this book. Imagine the author's surprise when, several years later, he personally experienced this same phenomenon when he grabbed the key to his 1967 Mustang by mistake and used it to start his 1990 Mustang without any trouble. Evidently, Ford hadn't changed their key pattern in 25 years.

This case study shows how the assumptions people make about security are often wrong, and that relying on a single security factor can be insufficient. People think that keys make their cars secure, and that's not always true, because not all manufacturers have done a good job of implementing key-based security.

Consider the three *D*s of security in the context of your own home, as an example. What would you do if you had something valuable (such as a diamond ring) that you wanted to protect while providing controlled access? You would want to use all three aspects of security. For defense, you would lock your doors and use key management technology, such as a locking key holder (you would never hide the key under the doormat or a potted plant, right?), to allow access only to those you authorize to enter your home. For detection, you might install cameras, infrared sensors, and an alarm system to alert you (and an alarm monitoring company) the instant a breach occurs. For deterrence, you would expect your local police to enforce laws, you might employ a security company to drive around your neighborhood periodically, and you might use other methods to discourage the theft of your valuables, such as keeping dogs or other intimidating pets. Relying on only one of the three *D*s would not be enough to prevent theft of your valuable object. You need to do all of them.

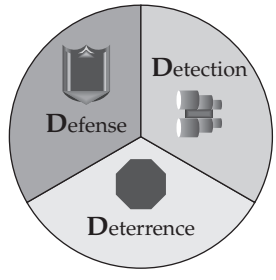

Figure 1-4 The three *D*s of security

Each of the three *D*s is equally important, and each complements the others, as represented in Figure 1-4. A defensive strategy keeps attackers at bay and reduces internal misuse and accidents. A detective strategy alerts decision makers to violations

of policy and other security events. And a deterrent strategy discourages attempts to undermine the business goals and processes and keeps resources efficiently focused on productive efforts. No security effort can be fully effective without all of these. Conversely, a security effort that employs all three *D*s provides strong protection.

CAUTION Do not employ only one or two of the three *D*s of security. All three aspects are necessary for an effective security program.

When only one or two of these aspects of security are applied to the network, *exposures* can result. A network that only uses defense and detection without deterrence is vulnerable to internal attacks, misuse, and accidents caused by employees who are not motivated to follow the correct procedures. A network that fails to employ detection faces exposure to all failures of the defensive and deterrent controls, and management may never become aware of these failures, which means abuses may continue unchecked. Of course, employing no defensive controls on a network exposes that network to any of the well-known threats of internal or external origin.

How to Build a Security Program

The overall approach to building a security program, as with any endeavor, should begin with describing what is needed and why, and to proceed to define how it will be implemented, when, and using which particular methods. There are many components that go into the building of a security program:

- **Authority** The security program must include the right level of responsibility and authorization to be effective.
- **Framework** A security framework provides a defensible approach to building the program.
- **Assessment** Assessing what needs to be protected, why, and how leads to a strategy for improving the security posture.
- **Planning** Planning produces priorities and timelines for security initiatives.
- **Action** The actions of the security team produce the desired results based on the plans.
- **Maintenance** The end stage of the parts of the security program that have reached maturity is to maintain them.

Figure 1-5 shows how a complete security program implementation would look in a midsize to large corporate environment. Smaller companies might simplify, streamline, or combine components depending on resource availability. These security program components, and how they fit together, are described in the following sections.

Authority

A security program *charter* defines the purpose, scope, and responsibilities of the security organization and gives formal authority for the program. Usually, the security organization

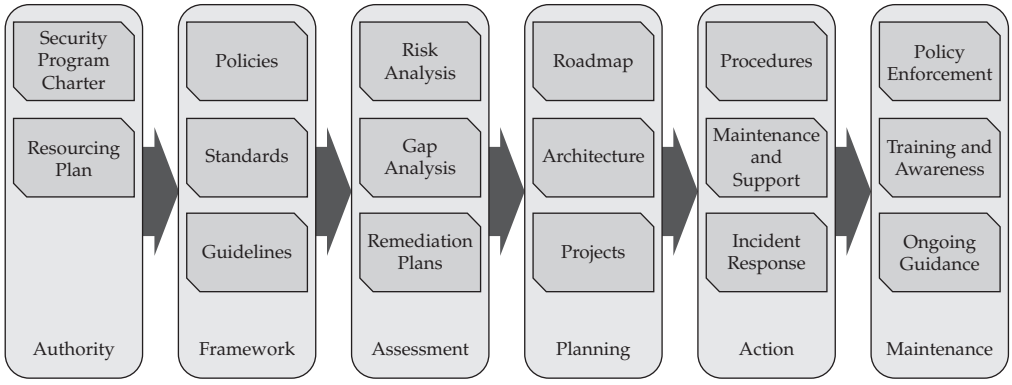

Figure 1-5 Security program components

is responsible for information protection, risk management, monitoring, and response. It might also be responsible for enforcement, such as reprimanding or even terminating employees or contract workers, but more commonly that authority is vested in the Human Resources department. Other responsibilities may include physical security, disaster-recovery and business-continuity planning, regulatory and internal compliance, and auditing. The set of responsibilities varies by company, but should be clearly specified in the security program charter, which should be authorized by the company's executive staff.

A resourcing plan is an ongoing strategy for providing the headcount needed to operate the security function. Insourcing, outsourcing, offshoring, and the like are factored into a resourcing plan, which describes how employees, contractors, consultants, service providers, and temporary workers will be leveraged to fuel the progress of security implementations, operations, and improvement. Chapter 6 covers the staffing of the security function.

Framework

The *security policy* provides a framework for the security effort. The policy describes the intent of executive management with respect to what must be done to comply with the business requirements. The policy drives all aspects of technical implementations, as well as policies and procedures. Ideally, a security policy should be documented and published before any implementations begin. The security policy represents business decisions about what to do based on certain assumptions. If the assumptions are not documented, they may be unclear or conflict with other activities. Documenting these assumptions in a clear, easy-to-read, accessible policy helps communicate expectations to everyone involved.

Standards are the appropriate place for product-specific configurations to be detailed. Standards are documented to provide continuity and consistency in the implementation and management of network resources. Standards change with each version of software and hardware, as features are added and functionality changes, and they are different for each manufacturer. Because standards do change, they require periodic revision to reflect changes in the software and hardware to which they apply.

Guidelines for the use of software, computer systems, and networks should be clearly documented for the sake of the people who use these technologies. Guidelines are driven to some extent by the technology, with details of how to apply the tools. They are also driven by the security policy, as they describe how to comply with the security policy.

Assessment

A *risk analysis* provides a perspective on current risks to the organization's assets. This analysis is used to prioritize work efforts and budget allocation, so that the greater risks can receive a greater share of attention and resources. A risk analysis results in a well-defined set of risks that the organization is concerned about. These risks can be mitigated, transferred, or accepted. Chapter 2 covers risk analysis in more detail.

A *gap analysis* compares the desired state of the security program with the actual current state and identifies the differences. Those differences, or gaps, form a collection of objectives to be acted on over the course of a remediation effort to improve the organization's security posture to bring it in line with one or more standards, requirements, or strategies.

Remediation planning takes into account the risks, gaps, and other objectives of the security program, and puts them together into a prioritized set of steps to move the security program from where it is today to where it needs to be at a future point.

Planning

A *roadmap* is a plan of action for how to implement the security remediation plans. It describes when, where, and what is planned. The roadmap is useful for managers who need the information to plan activities and to target specific implementation dates and the order of actions. It is also useful for implementers who will be responsible for putting everything together. The roadmap is a relatively high-level document that contains information about major activities and milestones coming up in the next defined period of time (often some combination of quarters, one year, three years, five years, or a "rolling" period of time that advances periodically).

The *security architecture* documents how security technologies are implemented, at a relatively high level. It is driven by the security policy and identifies what goes where. It does not include product specifications or specific configuration details, but it identifies how everything fits together. A good tool for architecture documents is a block diagram—a diagram that shows the various components of a security architecture at a relatively high level so the reader can see how the components work together. A block diagram does not show individual network devices, machines, and peripherals, but it does show the primary building blocks of the architecture. Block diagrams describe how various components interact, but they don't necessarily specify who made those components, where to buy them, what commands to type in, and so on.

The *project plans* detail the activities of the individual contributors to the various security implementations. A good project plan opens with an analysis phase, which brings together all of the affected parties to discuss and review the requirements, scope, and policy. This is followed by a design phase, in which the architecture is developed in detail and the implementation is tested in a lab environment. After the design has been made robust, an initial test is performed to expose bugs and problems. The implementation phase is next, with the implementation broken into small collections of tasks whenever possible. Testing

follows implementation, after which the design is revised to accommodate changes discovered during testing. Upon completion, the implementation team should meet to discuss the hits and misses of the overall project in order to prepare for the next phase.

Action

Procedures describe how processes are performed by people on an ongoing basis to produce the desired outcomes of the security program in a repeatable, reliable fashion.

Maintenance and support are part of maintaining the ongoing operations of the security program and its associated technologies, as part of a normal lifecycle of planning, updating, reviewing, and improving.

The actions that should be taken when a security event occurs are defined in the *incident response plan.* Advance planning for what to do when security incidents occur helps shorten the response time and provides repeatable, reliable, and effective actions to limit the scope and damage of an incident. Chapter 33 covers incident response.

Maintenance

Policy enforcement is necessary to ensure that the intentions of management are carried out by the various people responsible for the behavior and actions defined in the security policies. Often, this enforcement is a shared effort between security management, company management, and Human Resources.

Security awareness programs are used to educate employees, business partners, and other stakeholders about what behaviors are expected of them, what actions they should take under various circumstances to comply with security policies, and what consequences may ensue if they don't follow the rules. As an educational tool, an awareness program can also be a great resource for helping people understand why they should want to follow the rules, and how security benefits them. Motivation can be an effective approach.

Ongoing guidance for business projects, daily operations, and general walk-up questions is an important part of a security program. After all, business situations change every day, and security should be considered in every situation. Someone should be available to advise the business on the best way to do things in a secure manner.

The Impossible Job

A universal truth of security, regardless of the application, is that the job of the attacker is always easier than the job of the defender. The attacker needs only to find one weakness, while the defender must try to cover all possible vulnerabilities. Figure 1-6 illustrates this concept. The attacker has no rules—the attacker can follow unusual paths, abuse the trust of the system, or resort to destructive practices. The defender must try to keep their assets intact, minimize damage, and keep costs down. To illustrate this point, let's return to the house analogy. Homeowners who want to protect their property must try to anticipate every attack that is likely to happen, while attackers can simply use, bend, break, or mutilate the house's defenses. In an extreme example, the attacker can cut through the exterior, break the windows, knock down the walls, or set the house on fire. Homeowners have the more difficult job, trying to protect their assets against all types of attack.

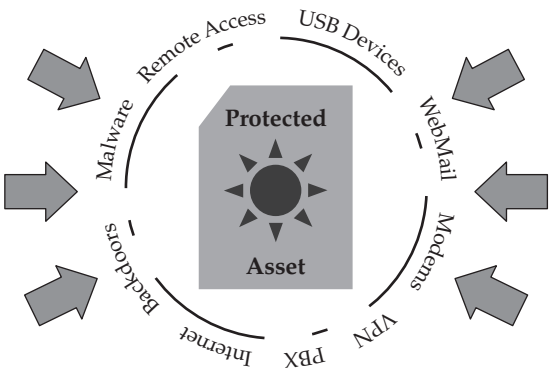

Figure 1-6 Attackers can choose their targets across the full attack surface.

In fact, the defender has an impossible job if the goal is to have 100 percent protection against all conceivable attacks. That is why the primary goal of security cannot be to eliminate all threats. Management may need to be educated about this concept, because they may not realize that this is a tenet of the security profession. Every defender performs a risk assessment by choosing which threats to defend against, which to insure against, and which to ignore. *Mitigation* is the process of defense, *transference* is the process of insurance, and *acceptance* is deciding that the risk does not require any action.

The Weakest Link

A security infrastructure will drive an attacker to the weakest link. For example, a potential burglar who is trying to break into a house may start with the front door. If the front door lock is too difficult to pick, the burglar may try side doors, back doors, and other entrances. If the burglar can't get through any of those, he may try to open a window. If they're all locked, he may try to break one. If the windows are unbreakable or barred, he may try to find other weaknesses. If the doors, windows, roof, and basement are all impenetrable, a determined burglar may try to cut a hole in the wall with a chainsaw. In what order will the burglar try these attacks? Usually, from the easiest to the hardest. The weakest link will attract the greatest number of attacks. Figure 1-7 demonstrates this concept.

All security controls should complement each other, and each should be equally as strong as the others. This principle is called *equivalent security* or *transitive security*.

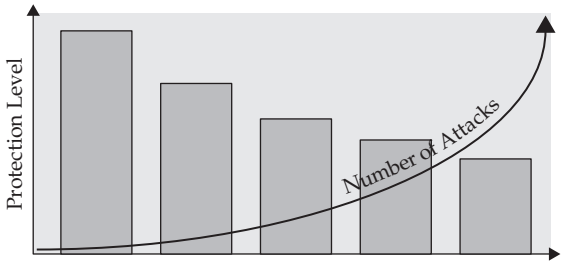

Figure 1-7 Attack vectors focus on the weakest link.

When you're deciding which security project should be your next priority, choose to shore up the weak points first. Because threats come from many sources and tend to focus on the weakest link, protecting a particular asset (for example, a credit card number) requires securing the asset as well as securing other resources (for example, servers, networks, databases, storage systems, printers, scanners, and fax machines) that have access to that asset. These resources may include nontechnical resources as well, so focusing only on electronic data can overlook important threat vectors.

For example, securing a credit card number should also include securing the system on which it resides, the network attached to that system, the other systems on the network, non-computer equipment (such as fax machines and phone switches) attached to that network, and the physical devices for each of these. It should also include securing the processes and procedures that affect that credit card number, such as system administration, backup tape rotation and handling, and background checks and hiring and termination procedures. Securing the data means discovering its path throughout the system, and protecting it at every point. If the credit card number is stored on the most secure network but a business process that prints the card numbers and stores them is kept in an unlocked room, the attacker will exploit this weakest link. Equivalent or transitive security controls on all the places where that asset may be attacked make the attacker's job harder by protecting against weak points the attacker can exploit.

In a computer network, firewalls are often the strongest point of defense. They encounter their fair share of attacks, but most attackers know that properly configured firewalls are difficult to penetrate, so they will look for easier prey. This can take the form of DSL lines in labs or small offices that aren't firewalled, modems and other remote access systems, Private Branch Exchange (PBX) phone switches, home computers and laptops that are sometimes connected to the company network, unpatched web servers and other Internet-facing servers, e-mail servers (to launch attacks such as *spear-phishing*), and Domain Name Service (DNS) servers that are accessible from the Internet. All of these typically offer less resistance to attackers than firewalls offer. That's why it's important for the security of these objects to be equally as strong as the firewall.

For any device that is to be protected, more attacks will occur via less protected paths, and those attacks will typically be more often successful. These attacks may exploit vulnerabilities in Internet-facing systems, compromised internal systems, administrative channels, unsecured paths, or even trusted credentials. The most successful of those attacks will be the ones that take advantage of the weakest security. Spending your limited time and money on improving the security of the firewall, the server, or the database may not be as effective as focusing on greater weaknesses.

One objective of an effective security strategy is to force the attacker to spend so much time trying to get past the defenses that he will simply give up and go elsewhere. Other strategies attempt to delay the intruder for a long enough time to take a reactive response, such as summoning authorities. Still others try to lure the attacker into spending too much time on a dead end.

In any case, weak points in the security infrastructure should be avoided whenever possible. In situations where weak points are necessary due to business requirements, detective and deterrent security controls should focus on the areas where defensive weak points exist. You can expect these weak points to attract attackers, and you should plan accordingly.

Strategy and Tactics

A *security strategy* is the definition of all the architecture and policy components that make up a complete plan for defense, detection, and deterrence. Security *tactics* are the day-to-day practices of the individuals and technologies assigned to the protection of assets. Put another way, strategies are usually proactive and tactics are often reactive. Both are equally important, and a successful security program needs to be both strategic and tactical in nature. With a well-defined strategic plan driving tactical operations, the security effort will have the best chance for success.

NOTE Dividing efforts between strategic (proactive) planning and tactical (reactive) operations can be challenging. However, both functions are equally important, and resources should be divided between the two. In extremely active environments, it can be helpful to set aside time each week for planning sessions that focus on the longer term.

Strategic planning can proceed on weekly, monthly, quarterly, and yearly bases, and should be considered an ongoing endeavor. Often there is an immediate need to secure a part of the network infrastructure, and time is not on the side of the strategic planner. In these cases, a tactical solution can be put in place temporarily to allow appropriate time for planning a longer-term solution.

In gauging the effectiveness of a security endeavor, separating strategy from tactics provides a way to focus on how business resources are being deployed. If a company finds itself focusing only on strategy or only on tactics, it should review its priorities and consider adding additional staff to address the shortfall.

Figure 1-8 demonstrates the interplay of strategy and tactics. Initially, at a given starting point in time, tactical effort may be high where strategy has not previously been employed. As time progresses and strategic planning is employed, tactical operations should begin to require less effort, because the strategy should simplify the operation and the business processes. This simplification is caused by the organization and planning provided by the strategic efforts, which reduce uncertainty and duplication of work by providing a proactive framework for staff to operate in. Given enough time, strategic planning should encompass tactics, confining them to the point where most daily tactical operations take place in a well-planned strategic context, and only unexpected fluctuations cause reactive efforts.

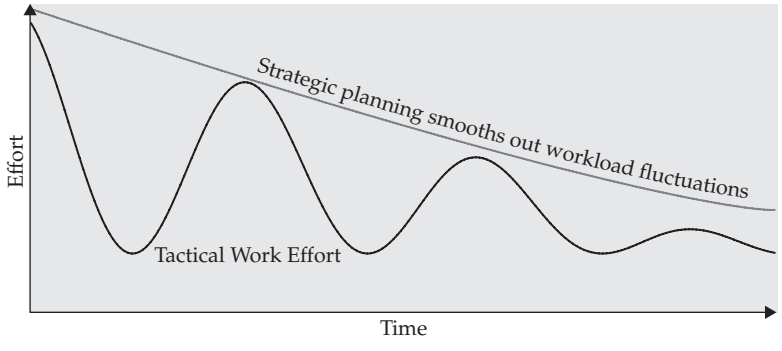

Figure 1-8 Strategy reduces tactical work effort over time.

In the ideal situation, strategy and tactics are at equilibrium. The strategic focus paves the way for quarter-to-quarter activities, and the tactical operations follow the strategy set forth in the previous quarters. In this balanced system of planning and action, a framework has been set in advance by the strategists for the operational staff to follow, which greatly facilitates the jobs of the operational staff who must react to both expected and unplanned situations. Instead of spending time figuring out how to respond to day-to-day situations, the operational staff follows a largely preplanned set of responses and implementations, leaving them free to cope with unexpected problems. In the network security context, this allows a better focus on incident response, virus control, correction of policy violations, optimization of implementations, and the like. For example, the tactical security practitioner can be freer to respond to an unexpected attack when incident response procedures and technologies have been planned in advance, instead of reacting on the fly and wasting valuable time during a crisis.

Business Processes vs. Technical Controls

In security, there is no *magic bullet*. In this sense, a magic bullet means a single security device, product, or technology that provides complete protection against all threats. Some security products are marketed as "security-in-a-box" solutions that provide all the security a company needs. In reality, security threats and exposures are complex and constantly evolving. Security technologies need to be selected on the basis of business context, so they are targeted toward specifically identified risks with clear objectives.

Organizations that place technical controls on their network without accompanying business processes have not recognized that computers are tools for accomplishing specific objectives, and that tools should be considered within a business process in order to be effective. For example, purchasing a database does not solve the problem of how to manage customer data. Customer data management is a business process that can be facilitated by a database. Likewise, buying a firewall doesn't magically provide security. Furthermore, if technical controls get in the way of the business or slow down workflow, people will find ways to work around them, rendering them ineffective or useless.

CAUTION There is a clear distinction between processes and tools. Often, the tools only support a limited set of processes, and in these situations, the processes may have to conform to the limitations of the tools. However, the tools only automate the processes; they do not define them or make them secure in and of themselves.

In the context of network security, business objectives, priorities, and processes determine the choice of tools, and the tools are used to facilitate the business processes. Figure 1-9 illustrates this principle. Any security implementation is a snapshot that includes the current threat model, the protection requirements, the environment being protected, and the state of the defensive technology at the time. As technology and the business environment evolve over time, the technical controls that are part of this snapshot will become less and less appropriate.

Before selecting security products, the business processes must be identified so that security products can be chosen that fit appropriately into the business environment. Proper consideration of how the security tools will be used to facilitate the business

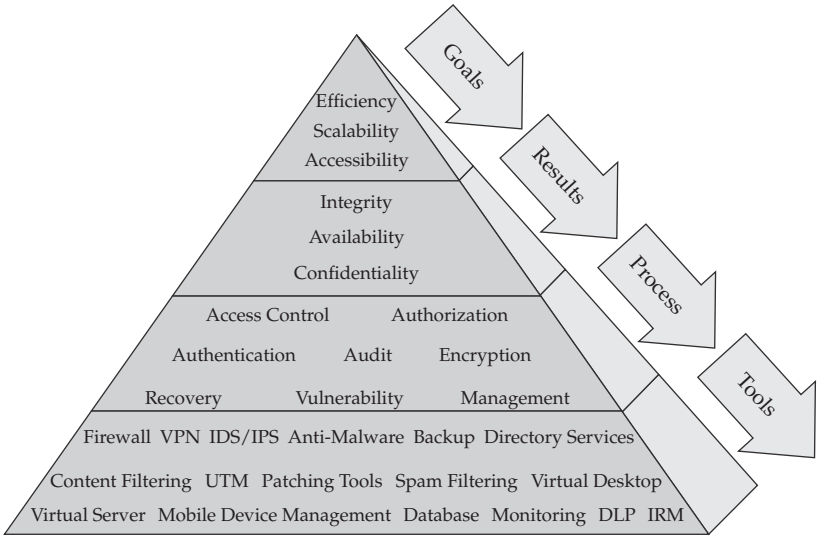

Figure 1-9 Business objectives, priorities, and processes drive tool selection.

requirements improves the likelihood that the security tools will remain effective and adequate. The security practitioner must attempt to understand the underlying business processes and data flows in order to solve the security challenge. This requires time and effort, but it's necessary for success. And the sooner the security practitioner is included in the project planning process, the more successful the security solution will be.

Make these assumptions when considering security:

- You can never be 100 percent secure.
- You can, however, manage the risk to your assets.
- You have many tools to choose from to manage risk. Used properly, these tools can help you achieve your risk management objectives.

Summary

Security implementations that solve specific business problems and produce results that are consistent with clearly identified business requirements produce tangible business benefits by reducing costs and creating new revenue opportunities. Companies that provide access into their network under control allow employees and customers to work together more effectively, enabling the business. Security both prevents unwanted costs and allows greater business flexibility. Thus security creates revenue growth at the same time as controlling losses.

Security can be thought of in the context of the three *D*s: defense, detection, and deterrence—each of which is equally important. Defense reduces misuse and accidents, detection provides visibility into good and bad activities, and deterrence discourages

unwanted behavior. A security program that employs all three *D*s provides strong protection and therefore better business agility (see Figure 1-5). Strategies are used to manage proactive security efforts, and tactics are used to manage reactive security efforts. Together, well-designed security strategy and tactics result in an effective, business-driven security program.

References

Byrnes, Christian F., and Dale Kutnick. *Securing Business Information: Strategies to Protect the Enterprise and Its Network*. Addison Wesley, 2002.

Gattiker, Urs E. *Information Security: Strategies for Understanding and Reducing Risks*. John Wiley & Sons, 2011.

Herrmann, Debra S. *A Practical Guide to Security Engineering and Information Assurance*. CRC Press, 2001.

Katsikas, Sokratis, and Dimitris Gritzalis, eds. *Information Systems Security: Facing the Information Society of the 21st Century*. Chapman & Hall, 1996.

McCumber, John. *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*. Auerbach Publications, 2004.

PricewaterhouseCoopers. "Eye of the Storm: Key Findings from the 2012 Global State of Information Security." Retrieved September 20, 2011, from www.pwc.com/giss2012.

Stackpole, Bill, and Eric Oksendahl. *Security Strategy: From Requirements to Reality*. Auerbach Publications, 2010.

Tipton, Harold F., and Micki Krause, eds. *Information Security Management Handbook*. Auerbach Publishing, 2001.

Tudor, Jan K. *Information Security Architecture: An Integrated Approach to Security in the Organization*. CRC Press, 2006.

Vladimirov, Andrew, Konstantin Gavrilenko, and Andriej Michajlowski. *Assessing Information Security: Strategies, Tactics, Logic and Framework*. IT Governance Publishing, 2010.

Wood, Charles C. *Best Practices In Internet Commerce Security*. Baseline Software, 2001.